How do we consider security at each stage of the Scrum process?

Plan	**Product Backlog Creation** Gather requirements from stakeholders and create user stories	• Agree on definition of what ‘secure’ means - test coverage, test types, language, • Educate team about security concerns for the product, security standards that need to be adhered to.
Design	**Sprint Planning and Sprint Backlog** Choosing which user stories to implement in the sprint and their priority, and defining the definition of done.	• Write acceptance tests • Carry out a security risk analysis for each of the stories • Specify definition of done for each story
Build	**Work on Sprint** Dev team writes solution for user stories	• Follow secure coding principles • Coding Rules – multiple reviewers on PRs • Have security sub-tasks for the code review • Write unit tests
Test	**Test and Demo** User stories are tested and the solution demoed to the PM for sign-off	• Automated security testing (using vulnerability identification software) • Pen-testing of new features • Write functional tests • Write integration tests
Deploy	**Deploy** The code is compiled, packaged and deployed for consumption by customers	• CI pipeline including security testing (like Checkmarx) • SOC compliance – list of requirements to prove that you are following security best practices – signed off by EM, PM, UX etc. • Black-box pentesting on live site
Review	**Sprint Retro** Look back at the work completed focussing on things that went well and things that could be improved for the next sprint	• Identify bugfixes that happened during the sprint - try to identify why they happened - implement change to avoid repeat of same issues in future sprints.